PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G11B 20/00, G06F 1/00

A1

(11) International Publication Number: WO 98/52194

(43) International Publication Date: 19 November 1998 (19.11.98)

(21) International Application Number: PCT/US98/09267

(22) International Filing Date: 6 May 1998 (06.05.98)

(30) Priority Data:
08/857,874 16 May 1997 (16.05.97) US

(71) Applicant: IMATION CORP. [US/US]; 1 Imation Place, P.O. Box 64898, Saint Paul, MN 55164-0898 (US).

(72) Inventor: BLIXT, Jon, J.; P.O. Box 64898, Saint Paul, MN 55164-0898 (US).

(74) Agents: LEVINSON, Eric, D. et al.; Imation Legal Affairs, P.O. Box 64898, Saint Paul, MN 55164-0898 (US).

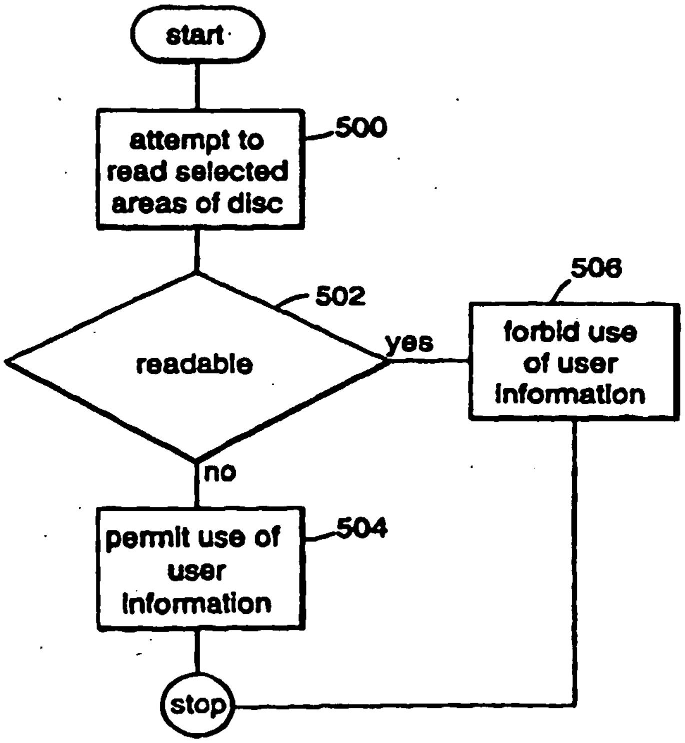
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: ARRANGEMENT AND METHOD FOR PREVENTING USE OF UNAUTHORIZED DUPLICATES OF DATA STORAGE MEDIA USING ADDRESS INFORMATION

(57) Abstract

A copy-protection method includes modifying address information (202, 204) on an optical disc (100). The modified address information (402) renders certain portions of the disc inaccessible and is not copied during typical copying operations. Storing user information (206) between the inaccessible portions prevents copying the user information to an unauthorized duplicate of the disc. Additionally, when a user wishes to use data stored on the disc, a disc reader optionally determines (502) whether the portions are accessible. If the portions are accessible (506), the user is prevented from using the data. If the portions are inaccessible (504), the user is permitted to use the data.


start
attempt to read selected areas of disc
500
502
readable
yes
506
forbid use of user information
no
permit use of user information
504
stop

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

ARRANGEMENT AND METHOD FOR PREVENTING USE OF UNAUTHORIZED DUPLICATES OF DATA STORAGE MEDIA USING ADDRESS INFORMATION

Field of the Invention

The present invention relates to data storage. More particularly, the present invention relates to preventing use of unauthorized copies of a data storage medium.

Background of the Invention

Optical media, such as discs recorded in the Compact Disc-Read Only Memory (CD-ROM) format, have become a popular data storage medium for storing computer software. Their large storage capacity allows them to store programs that are too large to be stored practically on certain other types of removable media, such as magnetic media known as floppy disks. For example, CD-ROMs are capable of storing video clips and CD-quality audio clips.

The proliferation of optical recording devices and writable optical media in the consumer market has facilitated storage of data on CD-ROMs. Decreasing prices of both optical recording devices and writable optical media have given an increasing number of consumers access to this technology. As a result, unauthorized duplication of CD-ROMs is a significant concern in the software industry.

Several techniques have been proposed to prevent unauthorized duplication of optical media. Some of these techniques involve using certain codes that identify an optical medium as an original. These techniques can be defeated using an approach known as sequential copying, in which the data on an optical medium is read sequentially and copied to a writable optical medium. Using sequential copying, an optical recording device can make a copy of an optical medium that is indistinguishable from the original. In addition, many such techniques involve using circuitry to detect the codes. Optical recording devices that lack this detection circuitry can copy optical media despite the presence of the codes.

Some other copy protection techniques involve physically altering the original medium to render areas of the medium difficult or impossible to read and copy by an optical reading device. An optical recording device can, however, copy the original medium by skipping over these areas. Because the original medium is physically altered, identifying the altered areas of the original medium is relatively easy. Furthermore, physical alterations may cause inconsistencies in playback from different optical reading device manufacturers. To prevent these inconsistencies, these techniques often use areas known as buffer zones to increase the error tolerance of the medium. These buffer zones use part of the user space on the medium and thus reduce the amount of space that can store other information.

Summary of the Invention

According to one embodiment, the present invention is directed to a method for use in preventing use of unauthorized duplicates of an original data storage medium storing user information. The method includes rendering certain portions of the data storage medium unreadable by modifying selected address information used for reading the data storage medium. Selected address segments of the data storage medium store the modified address and synchronization information. At least some of the user information is stored between the selected address segments. According to another embodiment of the present invention, a computer-executable program is stored on the original data storage medium. The computer-executable program, when executed, commands the data storage medium reading device to attempt to access the certain portions and determines whether to prevent or allow use of the user information as a function of whether the certain portions are inaccessible. Data recording apparatuses may perform these methods.

Still another embodiment of the present invention is directed to a data recording apparatus for use in preventing use of unauthorized duplicates of a data storage medium storing user information. An encoding arrangement is coupled to receive a data stream and configured and arranged to encode the data stream as a modulated data stream. A data processing arrangement is coupled to receive address information and is configured and arranged to modify the address information for rendering certain portions of the data storage medium inaccessible by a data storage medium reading device. An oscillator is configured and arranged to generate a laser beam. A modulator, responsive to a control signal, is configured and arranged to modulate the laser beam. A controller is responsive to the data processing arrangement and is configured and arranged to generate the control signal at least in part as a function of the modified address information.

Another embodiment of the present invention is directed to a data storage medium having a plurality of address segments storing address information altered to render certain portions of the data storage medium inaccessible by a data storage medium reading device. The data storage medium stores a computer-executable program. When executed, the computer-executable program commands the data storage medium reading device to attempt to access the certain portions and determines whether to prevent or allow use of user information stored on the data storage medium as a function of whether the certain portions are accessible.

According to another aspect of the present invention, an authentication method comprises commanding a data storage medium reading device to attempt to access certain portions of a data storage medium. The certain portions are inaccessible if the data storage medium is an original data storage medium, but are accessible if the data storage medium is an unauthorized duplicate of the original data storage medium. The authentication method also includes determining whether to prevent or allow use of user information stored on the data storage medium as a function of whether the certain portions are accessible.

The above summary of the invention is not intended to describe each disclosed embodiment of the present invention. This is the purpose of the figures and of the detailed description that follows.

Brief Description of the Drawings

Other aspects and advantages of the present invention will become apparent upon reading the following detailed description and upon reference to the drawings, in which:

FIG. 1 is a plan view of an optical data storage medium, according to the present invention, illustrating logical structures for storing data;

FIG. 2A is a diagram conceptually illustrating an example data format for storing data on the optical data storage medium of FIG. 1, according to the present invention;

FIG. 2B is a diagram conceptually illustrating another example data format for storing data on the optical data storage medium of FIG. 1, according to the present invention;

FIG. 3 is a block diagram of an optical recording device for recording data on the optical data storage medium of FIG. 1, according to the present invention;

FIG. 4 is a flow chart of a method for preventing unauthorized duplication of an optical data storage medium, according to the present invention; and

FIG. 5 is a flow chart of a method for authenticating an optical data storage medium, according to the present invention.

Detailed Description of the Various Embodiments

The present invention is believed to be applicable to a variety of systems and arrangements that prevent the use of unauthorized copies of optical storage media. The invention has been found to be particularly advantageous in application environments in which a CD-ROM or other optical medium stores user information, such as a computer-executable program for use by a personal computer (PC) or other computer arrangement. An appreciation of various aspects of the invention is best gained through a discussion of various application examples operating in such an environment. While the examples are discussed in the context of the CD-ROM format, it should be understood that the techniques described can be adapted readily to a variety of optical storage formats. Examples of such formats include, but are not limited to, the Digital Video Disc - Read Only Memory (DVD-ROM), CD-Erasable (CD-E), and CD-Recordable (CD-R) formats.

FIG. 1 illustrates a CD-ROM 100 that includes a reflective substrate on which information is stored as pits in the substrate and lands between the pits. The pattern of pits and lands represents the information stored on the CD-ROM 100. Any of a variety of techniques, including, for example, conventional photoresist techniques, can be used to create the pits.

The CD-ROM 100 includes a center aperture 102 to facilitate placement of the CD-ROM 100 in an optical reading device, such as a CD-ROM drive.

The CD-ROM 100 physically consists of a single spiral track from the inner perimeter of the CD-ROM 100 to the outer perimeter of the CD-ROM 100. While the spiral track is typically considered a single logical segment, the spiral track can be further divided into a plurality of logical segments 104, which are exaggerated on FIG. 1 for illustration purposes. The logical tracks 104 are further divided into sectors 106. The sectors 106 are also exaggerated on FIG. 1 for illustration purposes.

FIGS. 2A and 2B illustrate two example sector formats, according to the CD-ROM standard. In FIGS. 2A and 2B, the sectors are illustrated as subdivided into distinct sections for purposes of clarity. Those skilled in the art will appreciate that, in practice, the sections are typically interleaved to improve error tolerance. Interleaving involves dividing the sector into subunits known as frames and arranging the frames such that an error reading the disc is less likely to affect the data read from the disc catastrophically. In the CD-ROM format, the frames are twenty-four bytes long. Each CD-ROM frame is followed by a single byte of subcode data. The subcode bytes in a single sector combine to form a subcode section that contains certain format information.

FIG. 2A illustrates a sector format known as Mode 1. A Mode 1 sector includes twelve bytes comprising a synchronization section 202 and a four-byte header section 204. Together, the synchronization and header sections 202 and 204 contain address information used by a CD-ROM drive to locate data on the disc. The synchronization section 202 identifies the beginning of the sector. Three bytes of the header section 204 comprise an index known as absolute time or

ATIME. Absolute time identifies time indices from the beginning of the disc, e.g., using an internal clock of the optical reading device. One byte of the header section 204 indicates the type of data, e.g., program data, contained in the sector.

The header section 204 is followed by a user information section 206 that stores user information, such as program data, image data, or audio data. The user information section 206 is 2048 bytes long in a Mode 1 sector. The user information section 206 is followed by a four-byte error detection code (EDC) 208 and an eight-byte reserved section 210. The reserved section 210 is typically blank. A 276-byte error correction code 212 follows the reserved section 210 and provides enhanced error correction. An error detection/error correction (ED/EC) section 214 follows the error correction code 212 and provides basic error detection and correction functions. In the audio CD format, the formatting information includes time index and audio track, e.g., song, information.

FIG. 2B illustrates a CD-ROM sector format known as Mode 2. The Mode 2 format is similar to the Mode 1 format. In the Mode 2 format, however, the EDC section 208, the reserved section 210, and the ECC section 212 are absent. The space conserved by omitting these sections stores additional user information. Accordingly, the user information section 206 is 2336 bytes long in the Mode 2 format.

To prevent the use of software or other user information stored on an unauthorized copy of an original CD-ROM, according to the present invention, a manufacturer alters at least some of the synchronization and header sections on the CD-ROM. Modifying the synchronization and header sections renders certain portions of the CD-ROM difficult or impossible to read and copy. Accordingly, sequentially copying the CD-ROM is relatively difficult. The manufacturer can alter either a small or a large number of the synchronization and header sections.

After altering a small number of the synchronization and header sections, the manufacturer optionally stores an authentication program on the disc. The authentication program commands the CD-ROM drive to attempt to read the locations corresponding to the altered synchronization and header sections. If the disc is an original, the CD-ROM drive will be unable to read these locations. By contrast, an unauthorized copy of an original disc does not contain the altered synchronization and header sections, and the CD-ROM drive will successfully read the locations. Accordingly, the authentication program determines that the disc is an original and allows a user to use the disc if the CD-ROM cannot read the locations. Authenticating the CD-ROM as an original using an authentication program allows any CD-ROM drive to authenticate the CD-ROM. In addition, the authentication program prevents defeating the copy-protection by selectively copying user information and skipping the unreadable areas of the original CD-ROM.

As an alternative, the manufacturer can avoid using an authentication program by altering a large number of synchronization and header sections corresponding to relatively large areas of the disc. Altering more synchronization and header sections than the CD-ROM drive memory can store causes the CD-ROM drive to start and stop repeatedly when attempting to read these areas. Maintaining a sustained data rate for copying the disc is thus difficult, if not impossible.

FIG. 3 is a block diagram of an optical recording device, according to the present invention, used in producing a copy-protected CD-ROM. A digital data stream 300, such as program information for a computer application, is provided to an encoder 302.

For example, one type of encoder commonly used in recording data on CD-ROMs is known as an 8-to-14 modulation (EFM) encoder. Encoders of this type encode data streams having eight-bit bytes, which are commonly used to store data on magnetic media, to a data stream having fourteen-bit bytes. Optical storage media typically use fourteen-bit bytes to allow encoding of two consecutive ones using pits and lands. During read operations of a CD-ROM drive, an interface card converts the fourteen-bit code back to the eight-bit code used by the computer.

The encoder 302 provides the encoded data stream to a computer arrangement 306 that includes, for example, a CPU. The computer arrangement 306 is implemented using, for example, a conventional personal computer (PC) or a group of computers. A data processor 304 receives address information, *e.g.*, synchronization and header information, and modifies it. Modifying this information renders certain areas of the disc unreadable. For example, the synchronization and header information may be modified at multiple locations, between which user information is stored on the CD-ROM. Modifying the synchronization and header information at several locations and placing user information between these locations makes it difficult to maintain the sustained read rate involved in copying a CD-ROM by causing the CD-ROM drive to start and stop repeatedly as it attempts to read the user information.

The data processor 304 provides the modified synchronization and header information to the computer arrangement 306. The computer arrangement 306 then generates a recording signal based on the modified synchronization and header information and on the encoded data stream. It should be understood that the encoder 302 and/or the data processor 304 can either be separate from the computer arrangement 306, as described, or integrated into the computer arrangement 306. For example, the encoder 302 and the data processor 304 can be implemented using a single card installed on a computer.

A modulator controller 308 receives the recording signal and generates the control signal used for controlling a modulator 310. The modulator 310 modulates the intensity of a continuous-intensity laser beam generated by an oscillator 312. Accordingly, the modulator 310 produces a modulated laser beam having a modulation that varies as a function of the recording signal. An objective lens 314 focuses the modulated laser beam on a location of a CD-ROM or a master used for producing CD-ROMs.

FIG. 4 is a flow chart illustrating an example method for preventing use of unauthorized copies of an original CD-ROM, according to one embodiment of the present invention. As depicted at a block 400, an encoder reads source data, such as software code. The encoder provides this source data to a computer arrangement, which selectively alters synchronization and header information for at least some of the sectors of the CD-ROM to be recorded, as depicted at a block 402. At a block 404, the source data and the modified synchronization and header information are written to the CD-ROM. As depicted at a block 406, an authentication program is stored on the CD-ROM. The authentication program allows use of user information stored on the CD-ROM only if attempts to read particular portions of the CD-ROM produce read errors. Successfully reading the particular portions indicates that the CD-ROM does not contain the modified synchronization and header information and is therefore an unauthorized copy. Alternatively, the authentication program may be incorporated into another application program stored on the CD-ROM.

FIG. 5 is a flow chart illustrating an example of the operation of the authentication program. At a block 500 the authentication program commands the CD-ROM drive to read selected areas of the CD-ROM. The authentication program then determines whether the selected areas are readable, as depicted at a block 502. If the CD-ROM contains the modified synchronization and header information, the selected areas are unreadable. On the other hand, if the CD-ROM does not contain the modified synchronization and header information, attempts to read the selected areas are successful. Accordingly, as depicted at a block 504, if the selected areas of the CD-ROM are not readable, the authentication program permits use of user information stored on the CD-ROM. If, however, the selected areas are readable, the authentication program prevents the user from using the user information, as depicted at a block 506.

Modifying the synchronization and header information does not affect the manufacturing process. For example, the manufacturing process does not mistake these modifications as normal debris and does not attempt to correct for them by repairing the erroneous synchronization and header information. Furthermore, electrical testing of the CD-ROM does not reveal the modifications. The invisibility of the modifications to the manufacturing process renders circumventing the copy-protection difficult.

According to another embodiment of the present invention, a sufficient number of synchronization and header sections are altered to render sequentially reading and copying the disc difficult or impossible. By preventing sequential copying, this technique avoids the need for an authentication program. It should be understood, however, that this technique can be used with an authentication program or other copy-protection techniques for additional protection.

What is claimed is:

1. For use in preventing use of unauthorized duplicates of a data storage medium (100) storing user information, a copy-protection method comprising:

rendering certain portions of the data storage medium unreadable by modifying (402) selected address information (202,204) used for reading the data storage medium;

storing (404) the modified address information in selected address segments of the data storage medium; and

storing at least some of the user information (206) between the selected address segments.

2. The method of claim 1, further comprising:

commanding (500) a data storage medium reading device to attempt to access the certain portions; and

determining (502) whether to allow (504) or prevent (506) use of the user information as a function of whether the certain portions are accessible.

3. The method of claim 1, further comprising storing the user information and the address information in one of the following formats: DVD-ROM, CD-ROM, CD-E, and CD-R.

4. The method of claim 1, further comprising:

storing on the data storage medium a computer-executable program (406) that, when executed,

commands (500) a data storage medium reading device to attempt to access the certain portions, and determines (502) whether to prevent (506) or allow (504) use of the user information as a function of whether the certain portions are inaccessible.

5. For use in preventing use of unauthorized duplicates of a data storage medium (100) storing user information, a data storage apparatus comprising:

an encoding arrangement (302) coupled to receive a data stream (300) and configured and arranged to encode the data stream as a modulated data stream;

a data processing arrangement (304) coupled to receive address information and configured and arranged to modify (402) the address information (202,204) for rendering certain portions of the data storage medium inaccessible by a data storage medium reading device;

an oscillator (312) configured and arranged to generate a laser beam;

a modulator (310) responsive to a control signal and configured and arranged to modulate the laser beam; and

a controller (308) responsive to the microprocessor arrangement (306) and configured and arranged to generate the control signal at least in part as a function of the modified address information and the modulated data stream.

6. The apparatus of claim 5, wherein the encoding arrangement comprises an EFM encoder, and wherein the controller is further configured and arranged to generate the control signal in part as a function of the user information.

7. The apparatus of claim 5, wherein the data processing arrangement is further configured and arranged to command (308) the modulator to modulate the laser beam for storing an authentication program (406) on the data storage medium.

8. The apparatus of claim 7, wherein the authentication program comprises part of a computer-executable program and is configured and arranged to, when executed,

command the data storage medium reading device to attempt (500) to access the certain portions, and

determine (502) whether to prevent (506) or allow (504) execution of the computer-executable program as a function of whether the certain portions are inaccessible.

9. For use in preventing use of unauthorized duplicates of a data storage medium (100) storing user information, an authentication method comprising:

commanding a data storage medium reading device to attempt (500) to access certain portions of the data storage medium, the certain portions being inaccessible if the data storage medium is an original data storage medium and accessible if the data storage medium is an unauthorized duplicate of the original data storage medium; and

determining (502) whether to prevent (506) or allow (504) use of the user information as a function of whether the certain portions are accessible.

10. An optical data storage disc (100), comprising:

a plurality of address segments storing address information (202,204) altered to render certain portions of the data storage disc inaccessible by a data storage disc reading device; and

a computer-executable program (406) that, when executed,

commands the data storage disc reading device to attempt (500) to access the certain portions; and

determines (502) whether to prevent (506) or allow (504) use of user information stored on the data storage disc as a function of whether the certain portions are accessible.

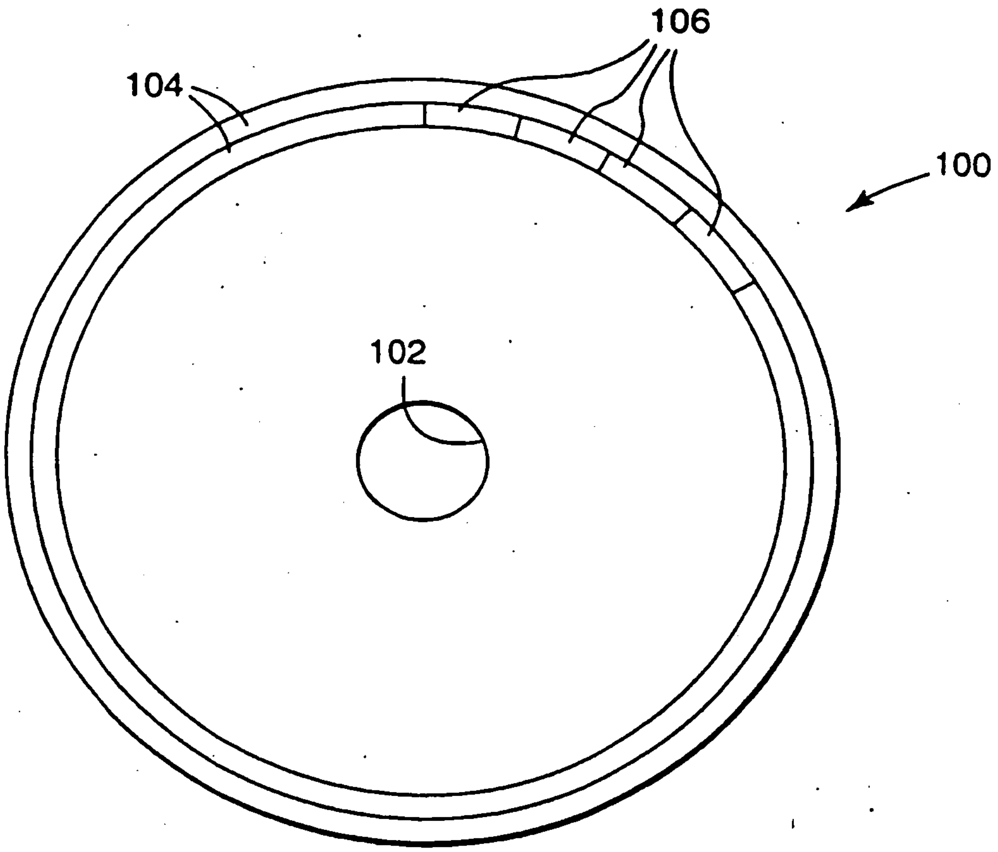
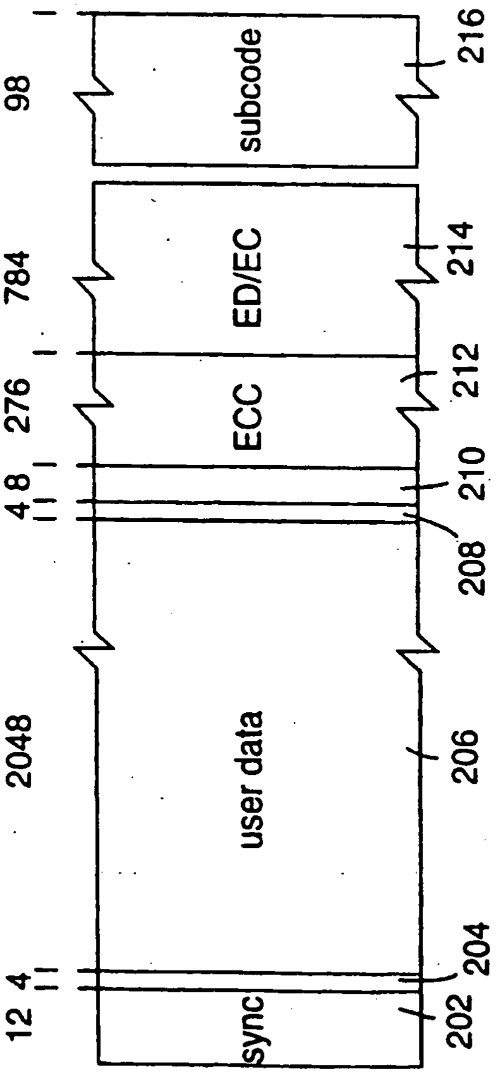


Fig. 1

Fig. 2A


12
4
2048
4
8
276
784
98
sync
user data
ECC
ED/EC
subcode
202
204
206
208
210
212
214
216

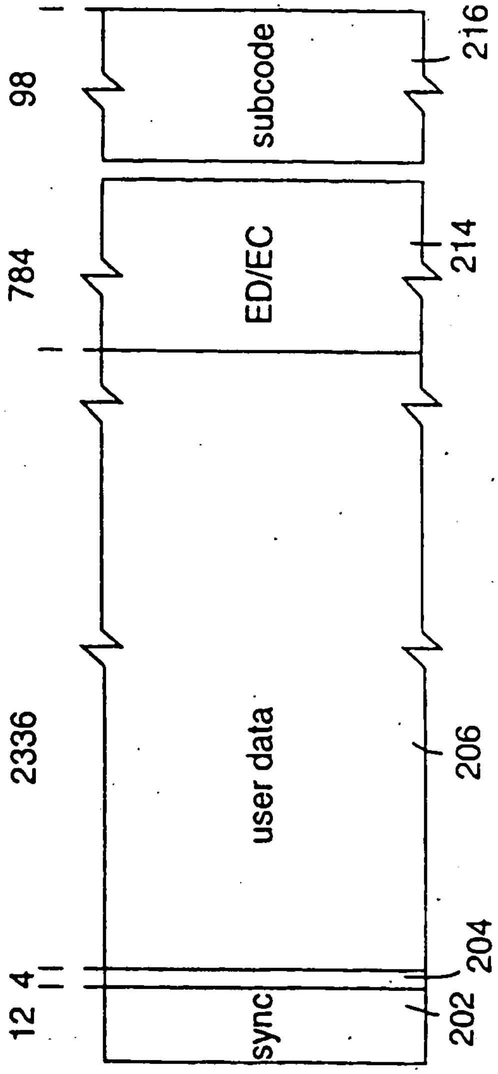

12
4
2336
784
98
sync
user data
ED/EC
subcode
202
204
206
214
216

Fig. 2B

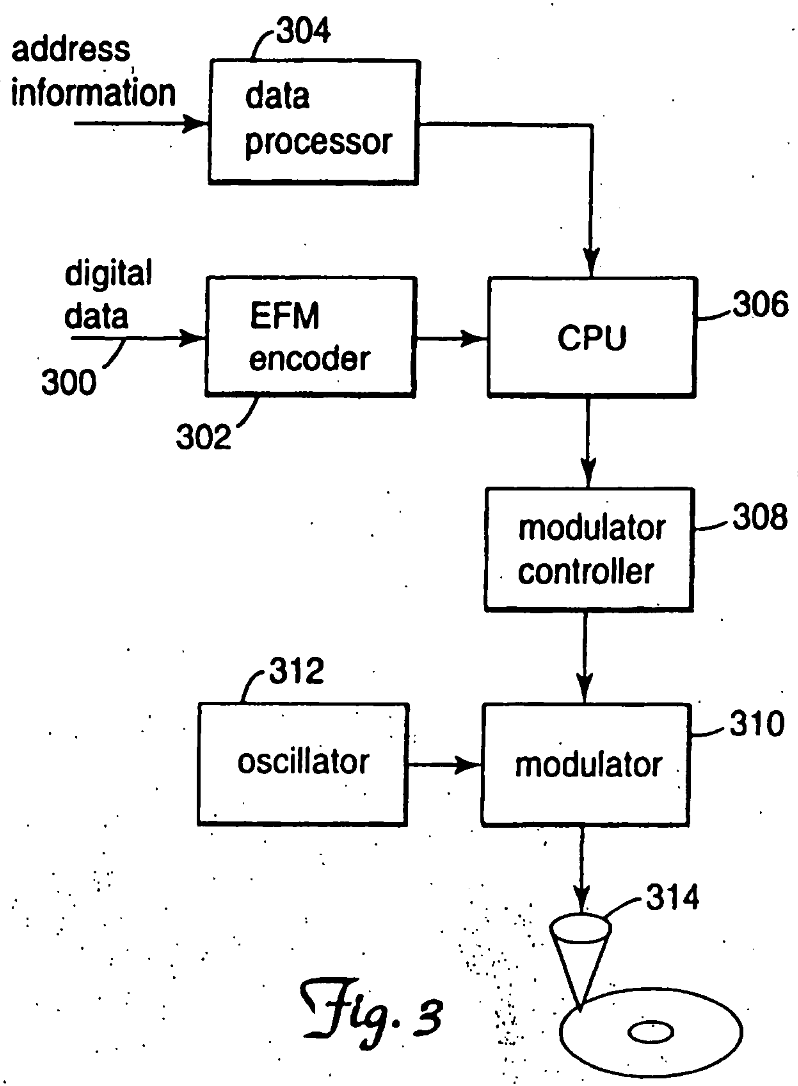

address information
304
data processor
digital data
300
EFM encoder
302
CPU
306
modulator controller
308
312
oscillator
modulator
310
314

Fig. 3

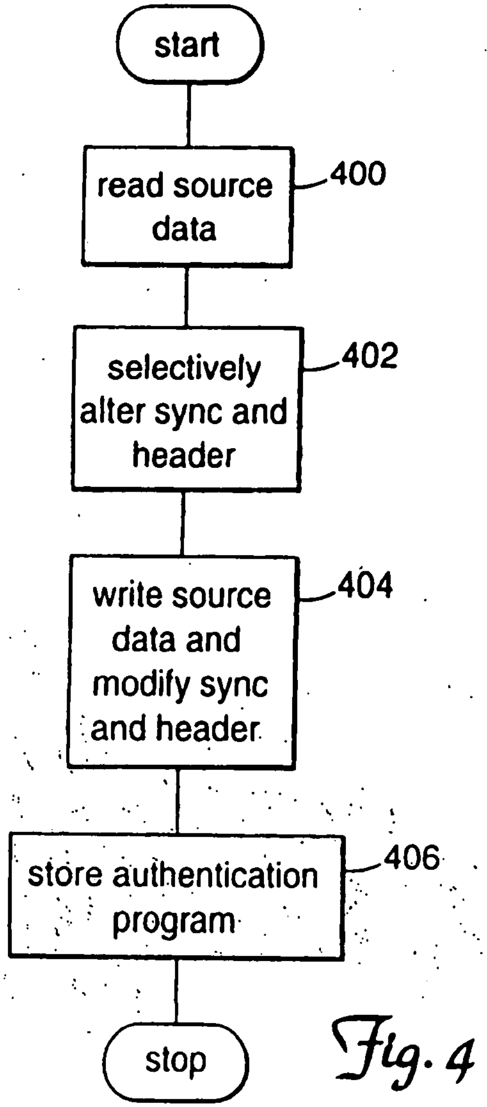

start
read source data
400
selectively alter sync and header
402
write source data and modify sync and header
404
store authentication program
406
stop

Fig. 4

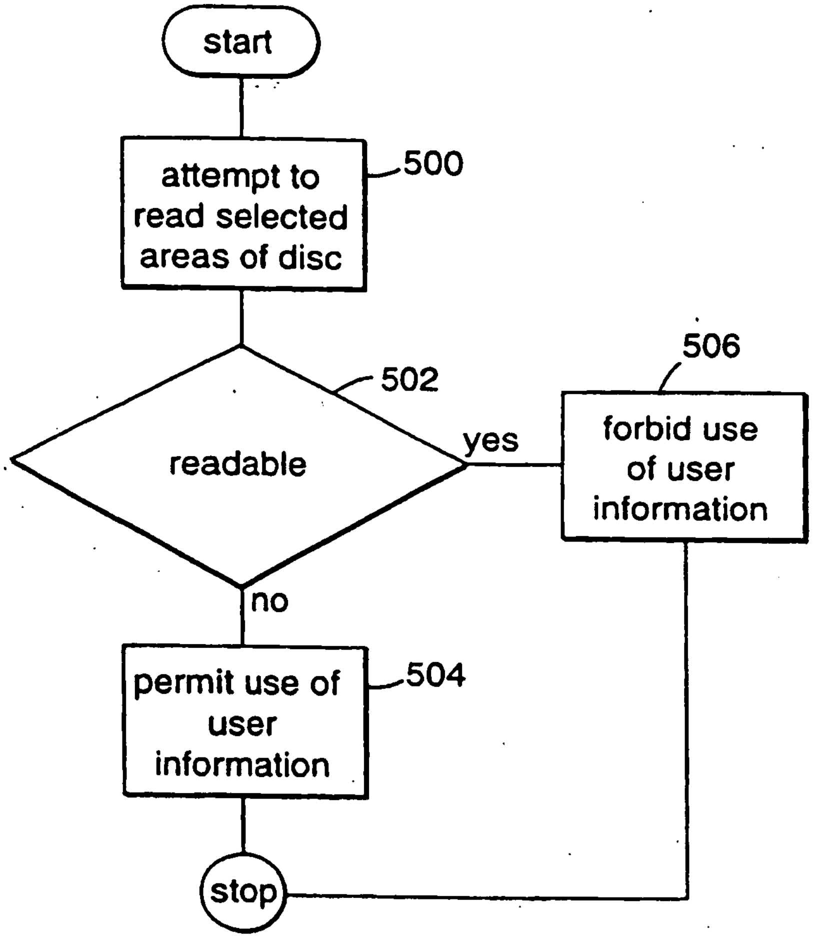

start
attempt to read selected areas of disc
500
readable
502
yes
no
forbid use of user information
506
permit use of user information
504
stop

Fig. 5